(5)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-162085
(43)Date of publication of application : 19.06.1998

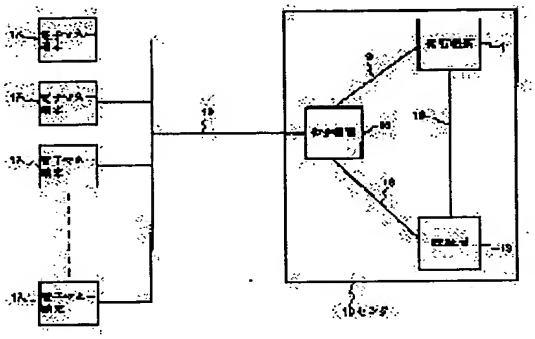
(51)Int.Cl. G06F 19/00
G07F 19/00
G07F 7/08
G09C 1/00
H04L 9/32

(21)Application number : 08-319146
(22)Date of filing : 29.11.1996

(71)Applicant : N T T DATA TSUSHIN KK
(72)Inventor : ICHIHARA NAOHISA
YABUMOTO TAKESHI

(54) ELECTRONIC MONEY SYSTEM, ELECTRONIC MONEY AND ELECTRONIC MONEY HISTORY GIVING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an electronic money system that can hold the anonymity of a history content added to an electric money, the electronic money and an electronic money history giving method.
SOLUTION: An issuing institution 11, a certification bureau 13 and a mediation institution 15 are respectively provided with secret keys. History initial information (r') obtained by combining the secret keys is added to the electronic money. An electronic money terminal 17 receiving the electronic money converts history initial information (r') into history information (r) and transfers it to the other electronic money terminal 17. In the case of transfer from the other electronic money terminal 17, the electronic money terminal 17 adds its own user ID to the history information (r). For investigating the history of the electronic money, the mediation institution 15 subtracts the value of its own secret key from history information (r) of the returned electronic money and sends it to the issuing institution 11. The issuing institution 11 subtracts the value of the self-secret key from history information from the mediation institution 15, polynomial resolution is executed and the electronic money terminal to which the electronic money is transferred is specified.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平１０－１６２０８５

(43)公開日　平成１０年（１９９８）６月１９日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
G06F 19/00			G06F 15/30	360	
G07F 19/00			G09C 1/00	660	C
7/08			G07D 9/00	476	
G09C 1/00	660		G07F 7/08		Z
H04L 9/32			H04L 9/00	675	D

審査請求　未請求　請求項の数１８　ＯＬ　（全１４頁）

(21)出願番号　特願平８－３１９１４６

(22)出願日　平成８年（１９９６）１１月２９日

(71)出願人　０００１０２７２８
エヌ・ティ・ティ・データ通信株式会社
東京都江東区豊洲三丁目３番３号

(72)発明者　市原　尚久
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　薮本　剛
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

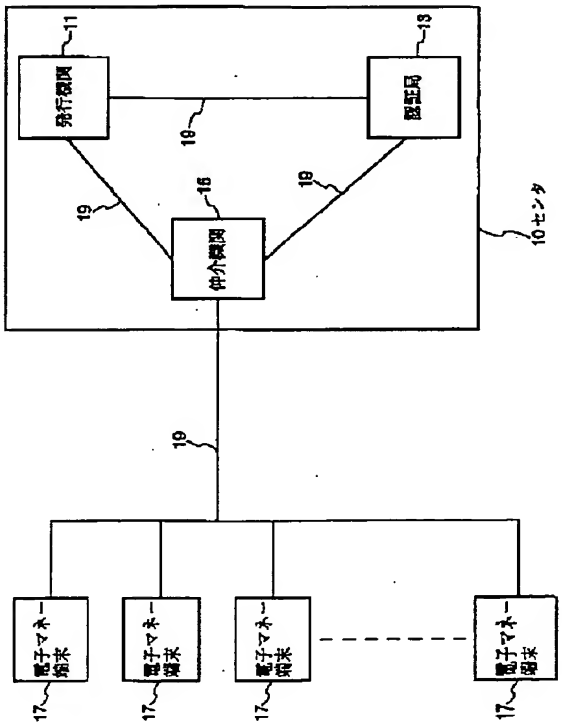
(74)代理人　弁理士　木村　満

(54)【発明の名称】電子マネーシステム及び電子マネー及び電子マネー履歴付与方法

(57)【要約】

【課題】　電子マネーに付された履歴内容の匿名性が保持可能な電子マネーシステム及び電子マネー及び電子マネー履歴付与方法を提供する。

【解決手段】　発行機関１１と認証局１３と仲介機関１５は、各自秘密鍵を備える。電子マネーには初めにそれらの秘密鍵を掛合わせた履歴初期情報ｒ'を付す。その電子マネーを受信した電子マネー端末１７は、所定式に従い、履歴初期情報ｒ'を履歴情報ｒに変換し、他の電子マネー端末１７に渡す。他の電子マネー端末１７からの譲渡の場合、電子マネー端末１７は、その履歴情報ｒに自己のユーザＩＤを加える。電子マネーの履歴を調査する場合、仲介機関１５は、戻されて来た電子マネーの履歴情報ｒから自己の秘密鍵の値を差し引き、発行機関１１に送る。発行機関１１は、仲介機関１５からの履歴情報から自己の秘密鍵の値を差し引き、多項式分解し、その電子マネーが譲渡された電子マネー端末を特定する。



1

【特許請求の範囲】

【請求項１】複数の端末を備え、該複数の端末間で電子マネーを授受する電子マネーシステムにおいて、

複数の鍵を用いて作成した履歴情報を前記電子マネーに付与し、前記端末に該電子マネーを供給するセンタを備え、

各前記端末には、自己を特定するための識別符号が付されており、

各前記端末は、

受信した電子マネーの送信元が前記センタか否かを判別する判別手段と、

前記判別手段により、前記受信した電子マネーの送信元が前記センタであると判別された場合、該電子マネーに付与された前記履歴情報を第１の所定式に従って変換することにより自己の前記識別符号を含ませる第１の更新手段と、

前記判別手段により、前記受信した電子マネーの送信元が前記センタではないと判別された場合、該電子マネーに付与された前記履歴情報に自己の前記識別符号を加える第２の更新手段と、を備え、

前記センタは、前記端末からの電子マネーに付与された前記履歴情報を前記鍵を用いて変換することにより、該電子マネーを授受した１つ又は複数の端末の識別符号の集合体を導出する導出手段と、前記１つ又は複数の端末の識別符号の集合体を各識別符号に分解する分解手段と、を更に備える、

ことを特徴とする電子マネーシステム。

【請求項２】前記センタから送信される電子マネーに付与されている前記履歴情報は、第１と第２と第３の鍵から構成されており、

前記端末の前記第１の更新手段は、前記センタからの前記履歴情報を前記第１の所定式に従って、前記第１と第２と第３の鍵のうちの２つの鍵と該端末の前記識別符号とより構成されるように更新する手段を備える、

ことを特徴とする請求項１に記載の電子マネーシステム。

【請求項３】前記センタの前記導出手段は、前記端末からの前記履歴情報に含まれる前記第１と第２と第３の鍵のうちの前記２つの鍵の値を減算することにより、前記１つ又は複数の端末の識別符号の集合体を導出する手段を備え、

前記分解手段は、前記導出手段により導出された前記１つ又は複数の端末の識別符号の集合体を多項式分解することにより、各識別符号に分解する手段を備える、

ことを特徴とする請求項２に記載の電子マネーシステム。

【請求項４】前記電子マネーには、該電子マネーが授受された端末の数を示すカウント情報が更に付与されており、

前記分解手段は、前記電子マネーに付与されている前記

2

カウント情報を用いて前記集合体を多項式分解する、

ことを特徴とする請求項３に記載の電子マネーシステム。

【請求項５】前記センタは、第１の鍵r_0を備える第１の制御手段と、第２の鍵r_1を備える第２の制御手段と、第３の鍵r_2を備える第３の制御手段と、前記第１と第２と第３の鍵から、数１で表される履歴情報ｒを算出する算出手段と、を備え、

前記端末に付与されている前記識別符号は２のべき乗値から構成され、

前記第１の所定式は、数２と数３を含み、

前記端末の前記第１の更新手段は、前記センタからの前記履歴情報ｒと数２に表すｇ（ｉ）をもとに数３に表す式に従ってｒを更新する手段を備えることにより、数４に表す履歴情報ｒを導出する、

ことを特徴とする請求項１に記載の電子マネーシステム。

【数１】$r = r_0 \times r_1 \times r_2$

【数２】$g(i) = b(r_2) \times (b(r_1) + b(r_0) + x(i) \times b(r_0) \times b(r_1))$

（$b(r_n)$はr_nの関数であり$r_n \times b(r_n) \bmod N = 1$を満たす。なお、Ｎは定数であり、Ａ ｍｏｄ Ｂは、ＡをＢで割った余りを示す。ｘ（ｉ）は、任意の端末ｉの識別符号を示す。）

【数３】$r = r \times g(i) \bmod N$

【数４】$r = r_0 + r_1 + x(i)$

【請求項６】前記センタは、電子マネーを発行する発行機関と、前記電子マネーに付与する履歴情報を生成する認証局と、前記端末に前記電子マネーを供給する仲介機関とから構成され、

前記発行機関は、前記仲介機関及び端末に秘密の鍵である第１の鍵r_0を備え、

前記仲介機関は、前記発行機関及び端末に秘密の鍵である第２の鍵r_1を備え、

前記認証局は、前記仲介機関及び発行機関及び端末に秘密の鍵である第３の鍵r_2備える、

ことを特徴とする請求項１乃至５のいずれか１項に記載の電子マネーシステム。

【請求項７】前記端末の前記第１の更新手段は、前記センタからの前記履歴情報を前記第１の所定式に従って、前記複数の鍵から少なくとも１つを除いたものと該端末の前記識別符号とより構成されるように更新する手段を備える、

ことを特徴とする請求項１に記載の電子マネーシステム。

【請求項８】複数の端末を備え、該複数の端末間で電子マネーを授受する電子マネーシステムにおいて、

複数の鍵の積からなる履歴情報を作成して電子マネーに付与し、前記端末に該電子マネーを供給するセンタを備え、

3

各前記端末には、自己を特定するための識別符号が付されており、

各前記端末は、

受信した電子マネーの送信元が前記センタか否かを判別する判別手段と、

前記判別手段により、前記受信した電子マネーの送信元が前記センタであると判別された場合、該電子マネーに付与された前記履歴情報を第１の所定式に従って変換することにより、前記複数の鍵の一部と自己の前記識別符号との和に変換する第１の更新手段と、

前記判別手段により、前記受信した電子マネーの送信元が前記センタではないと判別された場合、該電子マネーに付与された前記履歴情報に自己の前記識別符号を加える第２の更新手段と、を備え、

前記センタは、前記端末からの電子マネーに付与された前記履歴情報を前記鍵を用いて変換することにより、該電子マネーを授受した１つ又は複数の端末の識別符号の集合体を導出する導出手段と、前記１つ又は複数の端末の識別符号の集合体を各識別符号に分解する分解手段と、を更に備える、

ことを特徴とする電子マネーシステム。

【請求項９】前記センタから送信される電子マネーに付与されている前記履歴情報は、第１と第２と第３の鍵から構成されており、

前記端末の前記第１の更新手段は、前記センタからの前記履歴情報を前記第１の所定式に従って、前記第１と第２と第３の鍵のうちの２つの鍵と該端末の前記識別符号とより構成されるように更新する手段を備える、

ことを特徴とする請求項８に記載の電子マネーシステム。

【請求項１０】前記センタの前記導出手段は、前記端末からの前記履歴情報に含まれる前記第１と第２と第３の鍵のうちの２つの鍵の値を減算することにより、前記１つ又は複数の端末の識別符号の集合体を導出する手段を備え、

前記分解手段は、前記導出手段により導出された前記１つ又は複数の端末の識別符号の集合体を多項式分解することにより、各識別符号に分解する手段を備える、

ことを特徴とする請求項９に記載の電子マネーシステム。

【請求項１１】前記電子マネーには、該電子マネーが授受された端末の数を示すカウント情報が更に付与されており、

前記分解手段は、前記電子マネーに付与されている前記カウント情報を用いて前記集合体を多項式分解する、

ことを特徴とする請求項８乃至１０のいずれか１項に記載の電子マネーシステム。

【請求項１２】前記センタは、電子マネーを発行する発行機関の鍵と、前記電子マネーに付与する前記履歴情報を生成する認証機関の鍵と、前記端末に前記電子マネー

4

を供給する仲介機関の鍵と、の積からなる初期履歴情報を電子マネーに付与する手段を備え、

前記第１の所定式は、前記初期履歴情報を前記発行機関と前記仲介機関との鍵とその端末の前記識別符号の和に変換する式である、

ことを特徴とする請求項８乃至１１のいずれか１項に記載の電子マネーシステム。

【請求項１３】自己を特定するための識別符号が付されており、

電子マネーを受信する手段と、

受信した電子マネーの送信元を判別する判別手段と、

前記受信した電子マネーの送信元を電子マネーの供給元と判別した場合、該電子マネーに付与された履歴情報を第１の所定式に従って変換することにより、該履歴情報に自己の前記識別符号を含ませる第１の更新手段と、

前記受信した電子マネーの送信元を前記電子マネーの供給元以外であると判別した場合、該電子マネーに付与された前記履歴情報に自己の前記識別符号を加える第２の更新手段と、

電子マネーを送信する手段と、

を備える端末から構成されることを特徴とする電子マネーシステム。

【請求項１４】前記電子マネーの供給元からの電子マネーには、数５に示す履歴情報ｒが付与されており、

前記第１の所定式は、数６と数７を含み、

前記第１の更新手段は、前記履歴情報ｒと数６に表すｇ（ｉ）をもとに数７に表す式に従ってｒを更新する手段を備えることにより、数８に表す履歴情報ｒを導出する、

ことを特徴とする請求項１３に記載の電子マネーシステム。

【数５】$r = r_0 \times r_1 \times r_2$

ここで、r_0は電子マネーを発行する発行機関の鍵、ｒ１は前記電子マネーに付与する履歴情報を生成する認証局の鍵、ｒ２は前記端末に前記電子マネーを供給する仲介機関の鍵である。

【数６】$g(i) = b(r_2) \times (b(r_1) + b(r_0) + x(i) \times b(r_0) \times b(r_1))$

（$b(r_1)$はr_1の関数であり$r_1 \times b(r_1) \bmod N = 1$を満たす。なお、Ｎは定数であり、Ａ ｍｏｄ Ｂは、ＡをＢで割った余りを示す。ｘ（ｉ）は、任意の端末ｉの識別符号を示す。）

【数７】$r = r \times g(i) \bmod N$

【数８】$r = r_0 + r_1 + x(i)$

【請求項１５】前記電子マネーには、該電子マネーが授受された端末の数を示すカウント情報が更に付与されており、

前記端末は、受信した電子マネーに付されている前記カウント情報を更新する手段を含む、

ことを特徴とする請求項１３又は１４に記載の電子マネ

5

ーシステム。

【請求項１６】識別符号が付された複数の端末間で電子マネーを授受する電子マネーシステムにおいて、授受される電子マネーであって、

金銭的価値を有する情報と、

複数の鍵と該電子マネーが授受された端末の前記識別番号が含まれる履歴情報と、

該電子マネーが授受された端末の数をカウントするためのカウント情報と、より構成される、

ことを特徴とする電子マネー。

【請求項１７】識別符号が付された複数の端末間で電子マネーを授受する電子マネーシステムにおいて、授受される電子マネー取引の履歴を示す履歴情報を付与する電子マネー履歴付与方法であって、

複数の鍵を用いて作成した履歴情報を前記電子マネーに付与し、前記端末に該電子マネーを供給する供給ステップと、

前記端末が前記供給ステップより受信した前記電子マネーに付与された前記履歴情報を第１の所定式に従って該端末の識別符号を含むように変換する第１の更新ステップと、

前記端末が他の端末より受信した前記電子マネーに付与された前記履歴情報に該端末の識別符号を加える第２の更新ステップと、

前記端末からの前記電子マネーに付与された前記履歴情報を第２の所定式及び前記鍵を用いて変換することにより、該電子マネーが授受された１つ又は複数の端末の識別符号の集合体を導出するステップと、

前記１つ又は複数の端末の識別符号の集合体を各識別符号に分解するステップと、

を備えることにより前記電子マネーが授受された全ての前記端末を特定することができることを特徴とする電子マネー履歴付与方法。

【請求項１８】第１の鍵r_0を記憶し、要求に応じて前記第１の鍵r_0を前記供給ステップに送信する第１の送信ステップと、

第２の鍵r_1を記憶し、要求に応じて前記第２の鍵r_1を前記供給ステップに送信する第２の送信ステップと、

第３の鍵r_2を記憶し、要求に応じて前記第３の鍵r_2を前記供給ステップに送信する第３の送信ステップと、を更に有し、

前記供給ステップは、前記第１と第２と第３の鍵から、数９に示される履歴情報ｒを算出して、前記電子マネーに付与し、

前記第１の更新ステップは、前電子マネーに付与されている前記履歴情報ｒと数１０に表すｇ（ｉ）をもとに数１１に表す式に従ってｒを更新することにより、数１２に示す履歴情報ｒを導出する、

ことを特徴とする請求項１７に記載の電子マネー履歴付与方法。

6

【数９】$r = r_0 \times r_1 \times r_2$

【数１０】$g(i) = b(r_2) \times (b(r_1) + b(r_0) + x(i) \times b(r_0) \times b(r_1))$

（$b(r_i)$はr_iの関数であり$r_i \times b(r_i) \bmod N = 1$を満たす。なお、Ｎは定数であり、Ａ ｍｏｄ Ｂは、ＡをＢで割った余りを示す。ｘ（ｉ）は、任意の端末ｉの識別符号を示す。）

【数１１】$r = r \times g(i) \bmod N$

【数１２】$r = r_0 + r_1 + x(i)$

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子マネーに履歴を付けることが可能な電子マネーシステムに関し、特に電子マネーに付された履歴の内容の匿名性を維持可能な電子マネーシステム及び電子マネー及び電子マネー履歴付与方法に関する。

【０００２】

【従来の技術】近年、金銭的価値を有する電子マネーを用いた電子マネーシステムが提案されている。このようなシステムにおいて電子マネーの不正使用が発見された場合、その流通経路を追跡するため、電子マネーに履歴を付けることが望ましい。その一例として、電子マネーに利用者の識別符号（ＩＤ）、名前等を履歴として追加する方法が提案されている。しかし、この方法では、履歴を見ることにより、過去の使用者のＩＤ、名前等が知られてしまうため、電子マネーの匿名性という機能が失われてしまう。

【０００３】

【発明が解決しようとする課題】本発明は、上記実状に鑑みてなされたもので、履歴内容の匿名性が維持可能な電子マネーシステム及び電子マネー及び電子マネー履歴付与方法を提供することを目的とする。

【０００４】

【課題を解決するための手段】上記目的を達成するため、この発明の第１の観点に係る電子マネーシステムは、複数の端末を備え、該複数の端末間で電子マネーを授受する電子マネーシステムにおいて、複数の鍵を用いて作成した履歴情報を前記電子マネーに付与し、前記端末に該電子マネーを供給するセンタを備え、各前記端末には、自己を特定するための識別符号が付されており、各前記端末は、受信した電子マネーの送信元が前記センタか否かを判別する判別手段と、前記判別手段により、前記受信した電子マネーの送信元が前記センタであると判別された場合、該電子マネーに付与された履歴情報を第１の所定式に従って変換することにより自己の前記識別符号を含ませる第１の更新手段と、前記判別手段により、前記受信した電子マネーの送信元が前記センタではないと判別された場合、該電子マネーに付与された前記履歴情報に自己の前記識別符号を加える第２の更新手段と、を備え、前記センタは、前記端末からの電子マネー

に付与された前記履歴情報を第２の所定式及び前記鍵を用いて変換することにより、該電子マネーを授受した１つ又は複数の端末の識別符号の集合体を導出する導出手段と、前記１つ又は複数の端末の識別符号の集合体を各識別符号に分解する分解手段と、を更に備える。

【０００５】このような構成によれば、電子マネーが授受された端末の識別符号を履歴情報として電子マネーに付与することができる。その際、端末は電子マネーの送信元を判別し、送信元に応じた履歴情報の付与方法を用いる。これにより、その電子マネーの履歴情報の初期値が第１の更新手段により変換されるため、その端末に再度、同電子マネーが譲渡されてもその履歴情報を見ることができない。よって、匿名性が保持される電子マネーシステムを実現することができる。また、電子マネーがセンタに戻されたとき、センタは、その電子マネーに付与された履歴から、鍵を用いて、前記端末の識別符号の集合体を導出し、その集合体を分解することにより、その電子マネーが授受された全ての端末を特定することができる。

【０００６】前記センタから送信される電子マネーに付与されている前記履歴情報は、第１と第２と第３の鍵から構成されてもよく、前記端末の前記第１の更新手段は、前記センタからの前記履歴情報を前記第１の所定式に従って、前記第１と第２と第３の鍵のうちの２つの鍵と該端末の前記識別符号とより構成されるように更新する手段を備えてもよい。

【０００７】このような構成によれば、端末は、センタから供給された電子マネーに付与されている前記第１と第２と第３の鍵からなる履歴情報を、前記第１の所定式を用いることにより、２つの鍵と該端末の識別番号を付与した形に変換する。これにより、センタから初めに電子マネーを受け取った端末に、再度その電子マネーが譲渡されても、その端末は履歴内容を知ることができない。よって、匿名性が保持される電子マネーシステムを実現することができる。

【０００８】前記センタの前記導出手段は、前記端末からの前記履歴情報に含まれる前記第１と第２と第３の鍵のうちの２つの鍵の値を減算することにより、前記１つ又は複数の端末の識別符号の集合体を導出する手段を備えてもよく、前記分解手段は、前記導出手段により導出された前記１つ又は複数の端末の識別符号の集合体を多項式分解することにより、各識別符号に分解する手段を備えてもよい。例えば、前記電子マネーには、該電子マネーが授受された端末の数を示すカウント情報が更に付与されており、前記分解手段は、前記電子マネーに付与されている前記カウント情報を用いて前記集合体を多項式分解する。

【０００９】このような構成によれば、センタは端末からの履歴情報からその電子マネーが授受された端末の識別符号の集合体を導出し、その集合体をカウンタ情報を用いて多項式分解することにより、各識別符号に分解する。これにより、ある電子マネーが授受された全ての端末と、各端末にその電子マネーが譲渡された回数とを特定することができる。よって、その電子マネーの履歴を知ることができる。

【００１０】例えば、前記センタは、第１の鍵r_0を備える第１の制御手段と、第２の鍵r_1を備える第２の制御手段と、第３の鍵r_2を備える第３の制御手段と、前記第１と第２と第３の鍵から、数１３で表される履歴情報ｒを算出する算出手段と、を備え、前記端末に付与されている前記識別符号は２のべき乗値から構成され、前記第１の所定式は、数１４と数１５を含み、前記端末の前記第１の更新手段は、前記センタからの前記履歴情報ｒと数１４に表すｇ（ｉ）をもとに数１５に表す式に従ってｒを更新（置換）する手段を備えることにより、数１６に表す履歴情報ｒを導出する。

【数１３】$r = r_0 \times r_1 \times r_2$

【数１４】$g(i) = b(r_2) \times (b(r_1) + b(r_0) + x(i) \times b(r_0) \times b(r_1))$

（$b(r_n)$はr_nの関数であり$r_n \times b(r_n)$ ｍｏｄ Ｎ＝１を満たす。なお、Ｎは定数であり、Ａ ｍｏｄ Ｂは、ＡをＢで割った余りを示す。ｘ（ｉ）は、任意の端末ｉの識別符号を示す。）

【数１５】$r = r \times g(i) \bmod N$

【数１６】$r = r_0 + r_1 + x(i)$

【００１１】このような構成によれば、ある端末がセンタから受信した電子マネーを再度他の端末から受信し、その電子マネーの以前の履歴情報$r = r_0 \times r_1 \times r_2$を記憶していたとしても、履歴情報ｒが$r = r_0 + r_1 +$（ユーザＩＤの集合）と更新されており、$r_0 + r_1$の値が不明のため、履歴内容を知ることができない。よって、匿名性が保持される電子マネーシステムを実現することができる。

【００１２】例えば、前記センタは、電子マネーを発行する発行機関と、前記電子マネーに付与する履歴情報を生成する認証局と、前記端末に前記電子マネーを供給する仲介機関とから構成され、前記発行機関は、前記仲介機関及び端末に秘密の鍵である第１の秘密鍵r_0を備え、前記仲介機関は、前記発行機関及び端末に秘密の鍵である第２の秘密鍵r_1を備え、前記認証局は、前記発行機関及び仲介機関及び端末に秘密の鍵である第３の秘密鍵r_2備える。

【００１３】また、前記端末の前記第１の更新手段は、前記複数の鍵から構成される前記履歴情報を、該複数の鍵から少なくとも１つを除いたものと該端末の識別符号とより構成されるように更新してもよい。

【００１４】また、この発明の第２の観点に係る電子マネーシステムは、複数の端末を備え、該複数の端末間で電子マネーを授受する電子マネーシステムにおいて、複数の鍵の積からなる履歴情報を作成して電子マネーに付

与し、前記端末に該電子マネーを供給するセンタを備え、各前記端末には、自己を特定するための識別符号が付されており、各前記端末は、受信した電子マネーの送信元が前記センタか否かを判別する判別手段と、前記判別手段により、前記受信した電子マネーの送信元が前記センタであると判別された場合、該電子マネーに付与された前記履歴情報を第１の所定式に従って変換することにより、前記複数の鍵の一部と自己の前記識別符号との和に変換する第１の更新手段と、前記判別手段により、前記受信した電子マネーの送信元が前記センタではないと判別された場合、該電子マネーに付与された前記履歴情報に自己の前記識別符号を加える第２の更新手段と、を備え、前記センタは、前記端末からの電子マネーに付与された前記履歴情報を前記鍵を用いて変換することにより、該電子マネーを授受した１つ又は複数の端末の識別符号の集合体を導出する導出手段と、前記１つ又は複数の端末の識別符号の集合体を各識別符号に分解する分解手段と、を更に備える、ことを特徴とする。

【００１５】このような構成によれば、第１の所定式により、センタの鍵の一部が履歴情報から除去されるので、同電子マネーが再びこの端末に送信された場合でも、この端末は電子マネーの流通の履歴を判別することができない。従って、電子マネーの匿名性を維持することができる。

【００１６】前記センタから送信される電子マネーに付与されている前記履歴情報は、例えば、第１と第２と第３の鍵から構成されており、前記端末の前記第１の更新手段は、例えば、前記センタからの前記履歴情報を前記第１の所定式に従って、前記第１と第２と第３の鍵のうちの２つの鍵と該端末の前記識別符号とより構成されるように更新する。

【００１７】前記センタの前記導出手段は、例えば、前記端末からの前記履歴情報に含まれる前記第１と第２と第３の鍵のうちの２つの鍵の値を、該履歴情報から減算することにより、前記１つ又は複数の端末の識別符号の集合体を導出し、前記分解手段は、前記導出手段により導出された前記１つ又は複数の端末の識別符号の集合体を多項式分解することにより、各識別符号に分解する。

【００１８】前記電子マネーに、該電子マネーが授受された端末の数を示すカウント情報を付与し、前記分解手段は、前記電子マネーに付与されている前記カウント情報を用いて前記集合体を多項式分解するようにしてもよい。

【００１９】前記センタは、例えば、電子マネーを発行する発行機関の鍵と、前記電子マネーに付与する前記履歴情報を生成する認証機関の鍵と、前記端末に前記電子マネーを供給する仲介機関の鍵と、の積からなる初期履歴情報を電子マネーに付与する手段を備え；前記第１の所定式は、前記初期履歴情報を前記発行機関と前記仲介機関との鍵とその端末の前記識別符号の和に変換する式である。

【００２０】また、この発明の第３の観点に係る電子マネーシステムは、自己を特定するための識別符号が付されており、電子マネーを受信する手段と、受信した電子マネーの送信元を判別する判別手段と、前記受信した電子マネーの送信元を電子マネーの発行元と判別した場合、該電子マネーに付与された前記履歴情報を第１の所定式に従って変換することにより、該履歴情報に自己の前記識別符号を含ませる第１の更新手段と、前記受信した電子マネーの送信元を電子マネーの発行元以外と判別した場合、該電子マネーに付与された前記履歴情報に自己の前記識別符号を加える第２の更新手段と、電子マネーを送信する手段と、を備える、ことを特徴とする。

【００２１】このような構成によれば、電子マネーが授受される際、その電子マネーに履歴情報を付与することができる。また、このシステムでは、受信した電子マネーの送信元を判別し、送信元が電子マネーの発行元の場合、その電子マネーの履歴情報を第１の所定式に従って更新して送信する。これにより、その電子マネーの履歴情報の初期値が変わるため、再度、同電子マネーが譲渡されても、その履歴情報を見ることは不可能となる。よって、匿名性を保持した電子マネーシステムを実現することができる。

【００２２】例えば、電子マネーの供給元からの電子マネーには、数１７に示す履歴情報ｒが付与されており、前記第１の所定式は、数１８と数１９を含んでもよく、前記第１の更新手段は、前記履歴情報ｒと数１８に表すｇ（ｉ）をもとに数１９に表す式に従って前記履歴情報ｒを更新する手段を備えることにより、数２０に示す履歴情報ｒを導出するようにしてもよい。

【００２３】

【数１７】$r = r_0 \times r_1 \times r_2$

【数１８】$g(i) = b(r_2) \times (b(r_1) + b(r_0) + x(i) \times b(r_0) \times b(r_1))$

（$b(r_i)$はr_iの関数であり$r_i \times b(r_i) \bmod N = 1$を満たす。なお、Ｎは定数であり、Ａ ｍｏｄ Ｂは、ＡをＢで割った余りを示す。ｘ（ｉ）は、任意の端末ｉの識別符号を示す。）

【数１９】$r = r \times g(i) \bmod N$

【数２０】$r = r_0 + r_1 + x(i)$

【００２４】このような構成によれば、電子マネーの送信元が電子マネーの発行元である場合、前記第１の更新手段により、その電子マネーの履歴情報の初期値から秘密鍵r_2の値を差し引いた値が新たな履歴情報として電子マネーに付与される。これにより、その電子マネーの履歴情報の初期値が変わるため、再度、同電子マネーが譲渡されても、その履歴情報を見ることは不可能となる。よって、匿名性を保持した電子マネーシステムを実現することができる。

【００２５】また、この発明の第４の観点に係る電子マ

ネーは、識別符号が付された複数の端末間で電子マネーを授受する電子マネーシステムにおいて、授受される電子マネーであって、金銭的価値を有する情報と、複数の鍵と該電子マネーが授受された端末の前記識別番号が含まれる履歴情報と、該電子マネーが授受された端末の数をカウントするためのカウント情報と、より構成される。

【００２６】これにより、その電子マネーが授受された端末を特定することができる。

【００２７】また、この発明の第５の観点に係る電子マネー履歴付与方法は、識別符号が付された複数の端末間で電子マネーを授受する電子マネーシステムにおいて、授受される電子マネー取引の履歴を示す履歴情報を付与する電子マネー履歴付与方法であって、複数の鍵を用いて作成した履歴情報を前記電子マネーに付与し、前記端末に該電子マネーを供給する供給ステップと、前記端末が前記供給ステップより受信した前記電子マネーに付与された前記履歴情報を第１の所定式に従って該端末の識別符号を含むように変換する第１の更新ステップと、前記端末が他の端末より受信した前記電子マネーに付与された前記履歴情報に該端末の識別符号を加える第２の更新ステップと、前記端末からの前記電子マネーに付与された前記履歴情報を第２の所定式及び前記鍵を用いて変換することにより、該電子マネーが授受された１つ又は複数の端末の識別符号の集合体を導出するステップと、前記１つ又は複数の端末の識別符号の集合体を各識別符号に分解するステップと、を備えることにより前記電子マネーが授受された全ての前記端末を特定することができることを特徴とする。

【００２８】これにより、電子マネーが授受された端末の識別符号を履歴として付与することができる電子マネーシステムを実現することができる。また第１の更新ステップにより、その電子マネーの履歴情報の初期値が変換されるため、同端末に再度、同電子マネーが譲渡されてもその履歴情報を見ることができない。よって、匿名性が保持される電子マネーシステムを実現することができる。また、端末が電子マネーの送信元を判別し、送信元に応じた履歴の付与方法を用いることにより、センタに電子マネーが戻されたとき、所定の方法を用いて、その電子マネーが授受された全ての端末を特定することができる。

【００２９】第１の鍵r_0を記憶し、要求に応じて前記第１の鍵r_0を前記供給ステップに送信する第１の送信ステップと、第２の鍵r_1を記憶し、要求に応じて前記第２の鍵r_1を前記供給ステップに送信する第２の送信ステップと、第３の鍵r_2を記憶し、要求に応じて前記第３の鍵r_2を前記供給ステップに送信する第３の送信ステップと、を更に有してもよく、前記供給ステップは、前記第１と第２と第３の鍵から、数２１に示される履歴情報ｒを算出して、前記電子マネーに付与し、前記第１の更新ステップは、前電子マネーに付与されている前記履歴情報ｒと数２２に表すｇ（ｉ）をもとに数２３に表す式に従ってｒを更新することにより、数２４に示す履歴情報ｒを導出してもよい。

【００３０】

【数２１】$r = r_0 \times r_1 \times r_2$

【数２２】$g(i) = b(r_2) \times (b(r_1) + b(r_0) + x(i) \times b(r_0) \times b(r_1))$

（$b(r_n)$はr_nの関数であり$r_n \times b(r_n) \bmod N = 1$を満たす。なお、Ｎは定数であり、Ａ ｍｏｄ Ｂは、ＡをＢで割った余りを示す。ｘ（ｉ）は、任意の端末ｉの識別符号を示す。）

【数２３】$r = r \times g(i) \bmod N$

【数２４】$r = r_0 + r_1 + x(i)$

【００３１】これにより、前記供給手段より受信した電子マネーには、前記第１の更新ステップにより、その電子マネーの履歴情報の初期値から鍵r_2の値を差し引いた値が新たな履歴情報として付与される。これにより、電子マネーの履歴情報の初期値が変わるため、前記供給ステップから初めにその電子マネーを受信した端末が、再度、同電子マネーを受信しても、その履歴情報を見ることができない。よって、匿名性を保持した電子マネーシステムを実現することができる。

【００３２】

【発明の実施の形態】本発明の実施の形態に係る電子マネーシステムについて、以下図面を参照して説明する。この電子マネーシステムは、図１に示すように、電子マネーの発行機関１１と認証局１３と仲介機関１５とを備えるセンタ１０と、複数の電子マネー端末１７と、これらを接続する通信網１９より構成される。このシステムでは、発行機関１１により発行された電子マネーが仲介機関１５を介して利用者の電子マネー端末１７に供給され、利用者の電子マネー端末１７の間で電子マネーがやり取りされる形態をとる。

【００３３】発行機関１１は、この電子マネーシステム全体の動作、電子マネーの流通を制御（管理）するコンピュータを備え、電子マネーの発行、後述する履歴の調査等を行う。発行機関１１は、各電子マネー端末１７を特定するためのユーザＩＤのテーブルを記憶する。また、発行機関１１は、システム公開鍵Ｎを生成し、各利用者の電子マネー端末１７に通信網１９を介して配布する。認証局１３は、発行機関１１により発行された電子マネーに付与する履歴の初期情報（履歴初期情報）の生成等を行うコンピュータを備える。

【００３４】仲介機関１５は、例えば、金融機関等に設置され、発行機関１１との電子マネーの売買、利用者との電子マネーの売買等を行うコンピュータを備える。電子マネー端末１７は、利用者が仲介機関１５と電子マネーを売買し、他の利用者と電子マネーをやり取りするための端末である。各電子マネー端末１７は、システム公

開鍵Ｎ、ユーザＩＤ、履歴を更新するためのプログラム等を記憶する。また、発行機関１１はr_0、認証局１３はr_1、仲介機関１５はr_2をそれぞれ認証局１３を除く他者に秘密な鍵（秘密鍵）として保持する。なお、r_0とr_1とr_2は素数とする。

【００３５】本システムにおいて電子マネーの売買は通信を介して行われ、その精算方法は任意である。例えば、図２に示すように、このシステムの電子マネー端末１７と仲介機関１５と発行機関１１の決済口座を有する金融機関のコンピュータが通信網１９に接続されている。この金融機関のコンピュータが、電子マネーの売買が行われると、買い手の決済口座から売り手の決済口座へ売買された電子マネー相当の金額を振り替えるようにしてもよい。

【００３６】例えば、仲介機関１５が電子マネー端末17_1からの要求に応答して３万円分の電子マネーを送信した場合、金融機関のコンピュータは、電子マネー端末17_1の決済口座から仲介機関１５の決済口座へ３万円を振り替える。また、電子マネー端末17_2が仲介機関１５へ１万円分の電子マネーを送信した場合、金融機関のコンピュータは、仲介機関１５の決済口座から電子マネー端末17_2の決済口座へ１万円を振り替える。また、発行機関１１が仲介機関１５からの要求に応答して２０万円分の電子マネーを送信した場合、金融機関のコンピュータは、仲介機関１５の決済口座から発行機関１１の決済口座へ２０万円を振り替える。また、仲介機関１５が発行機関１１へ１０万円分の電子マネーを送信した場合、金融機関のコンピュータは、発行機関１１の決済口座から仲介機関１５の決済口座へ１０万円を振り替える。

【００３７】仲介機関１５が各利用者の電子マネー端末１７に供給する電子マネーの初期化処理について図３を参照して説明する。仲介機関１５は、例えば、予め一定額の電子マネーを発行機関１１から購入しておく。電子マネー端末１７は、仲介機関１５から電子マネーを購入したい場合、仲介機関１５に金額、ユーザＩＤ等を含む電子マネー購入要求を送信する。仲介機関１５は、この電子マネー購入要求に応答して、電子マネーに付与する履歴初期情報を作成するため、発行機関１１に秘密鍵r_0を認証局１３に送信するよう指示する（Ｌ１）と共に、自己の秘密鍵r_1を認証局１３に送信する（Ｌ２）。発行機関１１は、仲介機関１５からの指示を受けて、自己の秘密鍵r_0を認証局１３に送信する（Ｌ３）。なお、発行機関１１は、秘密鍵r_0を予め認証局１３に送信しておいても良い。

【００３８】認証局１３は、受信した秘密鍵r_0、r_1と自己の秘密鍵r_2をもとに、電子マネーに付与する履歴の初期情報である履歴初期情報$r' = r_0 \times r_1 \times r_2$を算出し、仲介機関１５に送信する（Ｌ４）。仲介機関１５は、受信した履歴初期情報r'と、電子マネーの利用者の数をカウントするためのカウンタ情報ｃ（初期値０に設定）とを、図４に示すように、発行機関１１により発行された電子マネーに付加する。これにより、電子マネーの初期化処理が完了する。初期化処理完了後、仲介機関１５は、履歴情報が付与された電子マネーを要求元の電子マネー端末１７に送信する。

【００３９】次に、各電子マネー端末１７における電子マネーに付加された履歴の更新処理について説明する。まず、前提として、各利用者の電子マネー端末17_i（$i = 1, 2, \cdots, m$（ｍは端末総数））が記憶するユーザＩＤを２のべき乗値である$x(i)$とし、電子マネー端末17_iが電子マネーを仲介機関１５から受信した際にその履歴初期情報r'を履歴情報ｒに更新するための更新式を$g(i)$とすると、それらは数２５、数２６の様に示される。

【００４０】

【数２５】$x(i) = 2^k$　（$k \geqq 0$）

【数２６】$g(i) = r_2^{-1} \times (r_1^{-1} + r_0^{-1} + x(i) \cdot r_0^{-1} \cdot r_1^{-1})$　（$1 \leqq i \leqq m$）

但し、任意の数をａとした場合、a^{-1}は、$a \cdot a^{-1} \bmod N = 1$を満たし、Ａ ｍｏｄ Ｂは、ＡをＢで割った余りを示す。

【００４１】まず、電子マネー端末17_iが、仲介機関１５から電子マネーを購入した場合、電子マネー端末17_iは、履歴情報ｒを数２７に従って算出し、カウンタ情報ｃを１カウントアップ（ｃ＝ｃ＋１）して、図５に示すように、電子マネーに付加する。

【００４２】

【数２７】$r = r' \times g(i) \bmod N$

これにより、仲介機関１５から電子マネー端末17_iに受け渡された電子マネーの履歴に、その電子マネー端末17_iのユーザＩＤを付加することができる。

【００４３】電子マネー端末17_iが、他の電子マネー端末１７から電子マネーを受け取った場合、電子マネー端末17_iは、その電子マネーに付与されている履歴情報ｒに自己のユーザＩＤである$x(i)$を足し込み、カウンタ情報ｃを１カウントアップする。即ち、電子マネー端末１７は、

（新たな履歴情報ｒ）＝（前回の履歴情報ｒ）＋$x(i)$

（新たなカウント情報ｃ）＝（前回のカウント情報ｃ）＋１

に従って計算し、その電子マネーの履歴を更新する。これにより、電子マネー端末17_iが、他の電子マネー端末１７から受け取った電子マネーの履歴に、その電子マネー端末17_iのユーザＩＤが付加される。

【００４４】仲介機関１５から受け取った電子マネーの履歴初期情報r'に、各電子マネー端末１７がユーザＩＤを加えていくだけの場合、最初に電子マネーを受け取る電子マネー端末１７が、その電子マネーの履歴初期情報r'を知ることができるため、再度その電子マネーを

15

受け取ったとき、その電子マネーの履歴内容を知ることができてしまう。

【００４５】例えば、図６に示すように履歴初期情報ｒ'＝１０の電子マネーが仲介機関１５から電子マネー端末１７ａに渡った場合、電子マネー端末１７ａは履歴初期情報ｒ'＝１０を記憶しておき、他の電子マネー端末１７ｂに渡す。その後も幾度かの譲渡を経て、再び電子マネー端末１７ａにその電子マネーが渡された場合、電子マネー端末１７ａは、受け取った電子マネーの履歴情報ｒから自己が記憶する履歴初期情報ｒ'＝１０を差

16

し引き、カウンタ情報ｃを用いて多項式分解することにより、その電子マネーを利用した利用者の電子マネー端末１７のユーザＩＤを知ることができてしまう。

【００４６】しかし、この発明の電子マネーシステムでは、電子マネー端末１７ｉが仲介機関１５から電子マネーを受け取った際に行う履歴情報ｒの算出式を展開すると数２８に示すようになる。

【００４７】

【数２８】

$$\begin{aligned} r &= r' \times g(i) \bmod N \\ &= r_0 \cdot r_1 \cdot r_2 \times r_2^{-1} \cdot (r_1^{-1} + r_0^{-1} + x(i) \cdot r_0^{-1}) \\ &= r_0 \cdot r_1 \cdot (r_1^{-1} + r_0^{-1} + x(i) \cdot r_0^{-1}) \\ &= r_0 + r_1 + x(i) \end{aligned}$$

【００４８】つまり、図７に示すように、最初に仲介機関１５から電子マネーを受け取った電子マネー端末１７ａが上記の式を用いて履歴情報を更新することにより、電子マネー端末１７ａがその後再びその電子マネーを受け取っても、$r_0 + r_1$の値がわからないため、履歴内容を知ることができない。これにより、電子マネーの匿名性を保持することができる。

【００４９】例えば、電子マネー端末１７から仲介機関１５に戻された電子マネーの不正使用が検出された場合、その電子マネーの流通経路を追跡するために、その電子マネーの履歴を調べる必要がある。このような場合での電子マネーの履歴の調査処理について、以下説明する。まず、仲介機関１５は、受信した電子マネーに付加されている履歴情報ｒから自己の秘密鍵r_1の値を差し引いた値（$r - r_1$）とカウンタ情報ｃを発行機関１１に送る。

【００５０】発行機関１１は、受信した電子マネーに付与された履歴情報（$r - r_1$）から自己の秘密鍵r_0の値を差し引き、カウンタ情報ｃを用いて多項式分解する。発行機関１１は、多項式分解により導出した分解要素集合を履歴Ｖとし、この履歴Ｖに含まれる各要素$v \in V$をユーザＩＤとして求める。

【００５１】発行機関１１の多項式分解処理について詳しく説明する。発行機関１１は、仲介機関１５から受信した履歴情報（$r - r_1$）から自己の秘密鍵r_0の値を更に差し引く。これにより、数２９に示すように、この電子マネーを利用した各利用者のユーザＩＤを足し込んだものが導出される。

【００５２】

【数２９】

$$\begin{aligned} r - r_1 - r_0 &= (r_0 + r_1 + x(i) + \cdots + x(n)) - r_1 - r_0 \\ &= x(i) + \cdots + x(n) \end{aligned}$$

なお、各ユーザＩＤｘ（ｉ）、・・・、ｘ（ｎ）は、２のべき乗値なので、数３０に示すように表せる。

【００５３】

【数３０】

$$x(i) + \cdots + x(n) = \sum_{h=0}^{n} a(h) \times 2^h$$

また、カウンタ情報ｃは、数３１に示すように表せる。

【００５４】

【数３１】

$$c = \sum_{h=0}^{n} a(h)$$

【００５５】数３０、数３１よりａ（ｈ）を一意に決定することができ、この各ａ（ｈ）が、この電子マネーを電子マネー端末17_1、・・・、17_nのそれぞれが受け取った回数となる。これにより発行機関１１は、「どの電子マネー端末１７が何回この電子マネーを受け取ったのか」を知ることができる。

【００５６】また、仲介機関１５に関しても、仮に仲介機関１５がその電子マネーの履歴初期情報ｒ'（＝$r_0 \times r_1 \times r_2$）を記憶していても、それから$r_0$を求めることはできないため、自己に渡された電子マネーの履歴を知ることはできない。よって、本システムでは、発行機関１１のみが仲介機関１５の協力を受けて電子マネーの履歴内容を知ることができる。

【００５７】発行された電子マネーが仲介機関１５から電子マネー端末１７に渡り、幾度かの譲渡を経て仲介機関１５に戻り、発行機関１１によってその履歴内容が導出されるまでの処理を図８を参照して具体的に説明する。例えば、端末数を３（電子マネー端末17_1、17_2、17_3）、秘密鍵$r_0 = 7$、秘密鍵$r_1 = 3$、秘密鍵$r_2 = 5$、システム公開鍵$N = 419$、とする。これらの条件により、$r_0^{-1} = 60$、$r_1^{-1} = 140$、$r_2^{-1} = 84$と決定され、ユーザＩＤであるｘ（ｉ）と、更新式であるｇ（ｉ）は表１に示す様に決定される。

【００５８】

【表１】

17　　18

電子マネー端末17_i	x（i）	g（i）
電子マネー端末17_1	x（1）＝1＝2^0	g（1）＝722400
電子マネー端末17_2	x（2）＝2＝2^1	g（2）＝1428000
電子マネー端末17_3	x（3）＝4＝2^2	g（3）＝2839200

【００５９】例えば、電子マネー端末１７$_3$が仲介機関１５に電子マネー要求信号を送信する（Ｓ０）。仲介機関１５は、この電子マネー要求信号に応答して、発行機関１１に秘密鍵を認証局１３に送信するよう指示する（Ｓ１）と共に、自己の秘密鍵r_1＝３を認証局１３に送信する（Ｓ２）。発行機関１１は、仲介機関１５からの指示に応答して、自己の秘密鍵r_0＝７を認証局１３に送信する（Ｓ３）。

【００６０】認証局１３は、自己の秘密鍵r_2＝５を用いて、履歴初期情報$r'=r_0\times r_1\times r_2=7\times3\times5=105$を計算し（Ｓ４）、仲介機関１５に送信する（Ｓ５）。仲介機関１５は、受信した履歴初期情報r'と、カウンタ情報ｃ＝０を電子マネーＭに付加する。

【００６１】仲介機関１５は、要求信号を受信すると、履歴初期情報r'とカウンタ情報ｃ＝０が付与された電子マネーＭを電子マネー端末１７$_3$に送信する（Ｓ６）。電子マネー端末１７$_3$は、仲介機関１５から電子マネーＭを受信し、その電子マネーＭに付与されている履歴初期情報r'とカウンタ情報ｃに対して、数３２と数３３に示す計算を行うことにより、履歴初期情報r'を履歴情報ｒに更新し、ｃを１カウントアップする（Ｓ７）。

【００６２】

【数３２】$r=r'\times g(2)\bmod N=105\times1428000\bmod419=12$

【数３３】ｃ＝０＋１＝１

【００６３】次に、電子マネー端末１７$_3$は、その電子マネーＭを電子マネー端末１７$_1$に譲渡することとする。電子マネー端末１７$_1$は、電子マネー端末１７$_3$から受信した電子マネーに付与されている履歴情報ｒとカウンタ情報ｃを数３４と数３５に示す様に更新する（Ｓ８）。

【００６４】

【数３４】$r=r+x(1)=12+1=13$

【数３５】ｃ＝１＋１＝２

【００６５】次に、電子マネー端末１７$_1$は、その電子マネーＭを電子マネー端末１７$_2$に譲渡することとする。電子マネー端末１７$_2$は、電子マネー端末１７$_1$から受信した電子マネーに付与されている履歴情報ｒとカウンタ情報ｃを数３６と数３７に示す様に更新する（Ｓ９）。

【００６６】

【数３６】$r=r+x(3)=13+4=17$

【数３７】ｃ＝２＋１＝３

【００６７】最後に、電子マネー端末１７$_3$は、その電子マネーＭを電子マネー端末１７$_2$に譲渡することとする。電子マネー端末１７$_2$は、電子マネー端末１７$_3$から受信した電子マネーに付与されている履歴情報ｒとカウンタ情報ｃを数３８と数３９に示す様に更新する（Ｓ１０）。

【００６８】

【数３８】$r=r+x(2)=17+2=19$

【数３９】ｃ＝３＋１＝４

【００６９】電子マネー端末１７$_3$は、電子マネーＭを換金するため仲介機関１５に送信する（Ｓ１１）。例えば、仲介機関１５が電子マネーＭを受信した際、不正検出等の理由により、その電子マネーＭの履歴を調べる必要が発生したとする。この場合、仲介機関１５は、電子マネーＭの履歴情報ｒから自己の秘密鍵r_1の値を差し引いて（$r=19-3=16$）（Ｓ１２）、電子マネーＭを履歴調査要求と共に発行機関１１に送信する（Ｓ１３）。

【００７０】発行機関１１は、受信した履歴調査要求に応答して、電子マネーＭの履歴情報ｒから自己の秘密鍵r_0の値を差し引いて、$r=16-7=9$と算出する。この算出結果が、電子マネーＭが譲渡された各電子マネー端末１７のユーザＩＤの集合となる。発行機関１１は、$r=9$とカウンタ情報ｃ＝４と自己が記憶するユーザＩＤテーブル（表１）を用いて数４０に示す様に多項式分解する（Ｓ１４）。即ち、ｒの値を、項数がｃで、各項の値がｘ（ｉ）のいずれかとなるように多項式分解する。

【００７１】

【数４０】$r=9=1+2+2+4$　表１より、ｘ（１）＝１、ｘ（２）＝２、ｘ（３）＝４なので、「この電子マネーＭは、電子マネー端末１７$_1$に１回、電子マネー端末１７$_2$に２回、電子マネー端末１７$_3$に１回譲渡されて仲介機関１５に戻ってきた」という履歴の調査結果が得られる。

【００７２】なお、各電子マネー端末１７のユーザＩＤであるｘ（ｉ）、更新式ｇ（ｉ）の取得方法は任意である。例えば、電子マネー端末１７がこのシステムのユーザ登録をする際に、発行機関１１が、その電子マネー端末１７に対して新たなユーザＩＤであるｘ（ｎ）を生成し、そのユーザＩＤであるｘ（ｎ）と自己の秘密鍵r_0を認証局１３に送信すると共に、仲介機関１５に秘密鍵r_1を認証局１３に送信するよう指示する。

【００７３】認証局１３は、受信した秘密鍵r_0、r_1と

ユーザＩＤであるｘ（ｎ）をもとに更新式ｇ（ｎ）を算出し、ユーザであるＩＤ（ｎ）とともに発行機関１１に送信する。発行機関１１は、通信網１９を介して、ユーザ登録する電子マネー端末１７にユーザＩＤであるｘ（ｎ）と更新式ｇ（ｎ）を送信する。電子マネー端末１７は、受信したユーザＩＤであるｘ（ｎ）と更新式ｇ（ｎ）を記憶する。

【００７４】上記説明では、３つの秘密鍵r_0、r_1、r_2を用いたが、秘密鍵の数はこれに限定されず任意である。

【００７５】なお、電子マネー端末１７の形態は任意であり、個人・商店の取引用端末（ＰＯＳ）、移動端末（モバイル端末）等でもよい。

【００７６】また、電子マネー端末１７は、着脱可能なＩＣカードを備えてもよく、このＩＣカードに、ユーザＩＤであるｘ（ｉ）、更新式ｇ（ｉ）、残高等を記憶してもよい。利用者が電子マネー端末１７を使用する時以外はこのＩＣカードを他の場所に保管しておくことにより、セキュリティを高めることができる。このとき、例えば、書き換え不可能な追記型の光記憶部と、ＩＣメモリ部とを備えたＩＣカードを用いてもよい。この場合、ＩＣメモリ部に残高等を記憶し、光記憶部に電子マネーのチャージ、支払い、譲渡、換金等の履歴を追記することが望ましい。

【００７７】なお、この発明の電子マネーシステムは、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、コンピュータに上述の動作を実行するためのプログラムを格納した媒体（フロッピーディスク、ＣＤ－ＲＯＭ等）から該プログラムをインストールすることにより、上述の処理を実行するコンピュータ及び端末を構成することができる。

【００７８】また、コンピュータにプログラムを供給するための媒体は、通信媒体（通信回線、通信ネットワーク、通信システムのように、一時的に流動的にプログラムを保持する媒体）でも良い。例えば、通信ネットワークの掲示板（ＢＢＳ）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、ＯＳの制御下で、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【００７９】

【発明の効果】以上説明したように、本発明によれば、端末が電子マネーを供給するコンピュータから電子マネーを受け取った際、その電子マネーに付与されている複数の秘密鍵からなる履歴情報を、複数の秘密鍵のうちのいくつかと該端末の識別番号より構成されるように変換させる。これにより、該端末が、再度その電子マネーを受け取っても、履歴内容を知ることができない。よって、匿名性が保持される電子マネーシステムを実現することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る電子マネーシステムの構成を示す図である。

【図２】電子マネーを売買する際の精算方法の一例を説明するための図である。

【図３】電子マネーの初期化処理を説明するための図である。

【図４】仲介機関により初期化処理された電子マネーの構成を示す図である。

【図５】電子マネー端末が仲介機関から受信した電子マネーに対して更新処理したときの電子マネーの構成を示す図である。

【図６】電子マネーの履歴初期情報に各電子マネー端末のユーザＩＤを加えていくだけの履歴の更新処理について説明するための図である。

【図７】本発明の電子マネーシステムにおける履歴の更新処理を説明するための図である。

【図８】発行された電子マネーが、複数の電子マネー端末間において譲渡され、仲介機関に戻され、発行機関によってその履歴内容が導出されるまでの処理を具体的に説明するための図である。

【符号の説明】

１１　発行機関
１３　認証局
１５　仲介機関
１７　電子マネー端末
１９　通信網

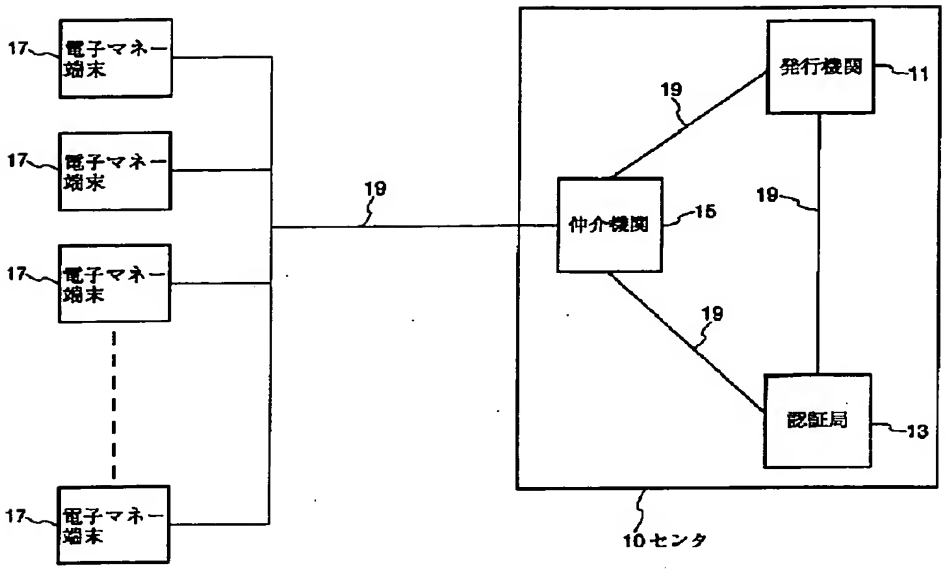
【図４】

電子マネー	履歴初期情報 $r=r_0 \times r_1 \times r_2$	カウンタ情報 c=0

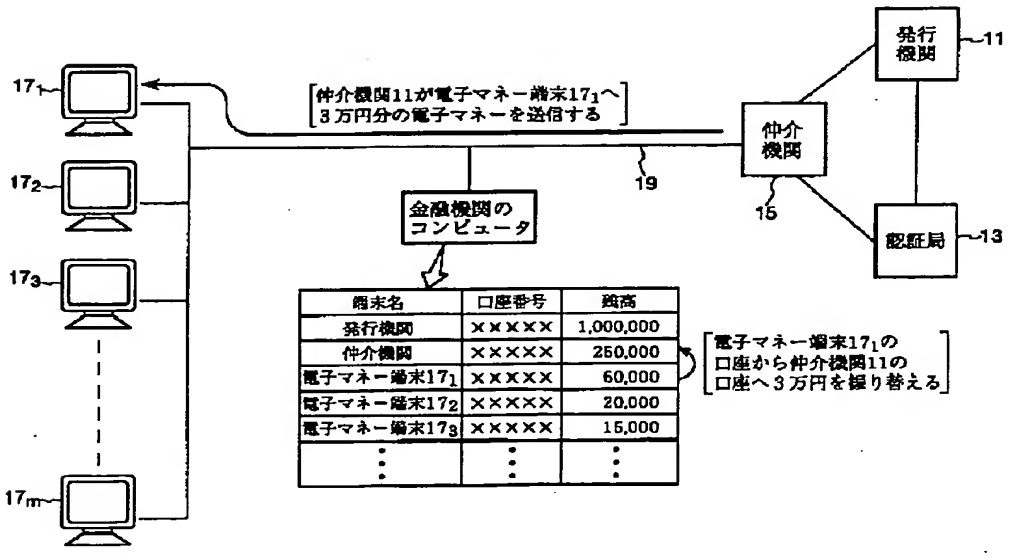
【図５】

電子マネー	履歴情報 $r=r' \times g(i) \bmod N$	カウンタ情報 c=1

【図１】

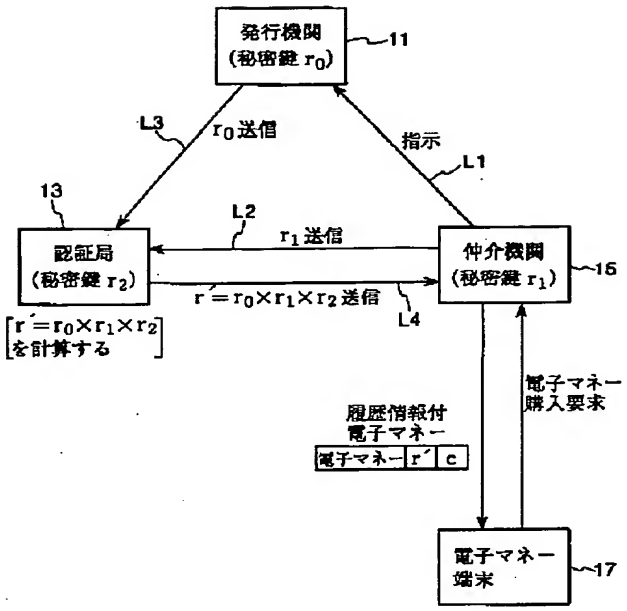


【図２】



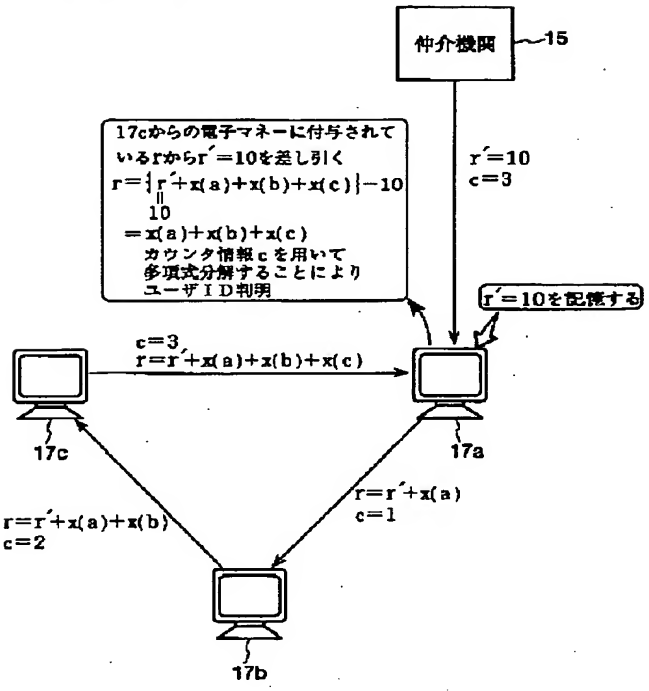
端末名	口座番号	残高
発行機関	×××××	1,000,000
仲介機関	×××××	250,000
電子マネー端末17₁	×××××	60,000
電子マネー端末17₂	×××××	20,000
電子マネー端末17₃	×××××	15,000
⋮	⋮	⋮

【図３】

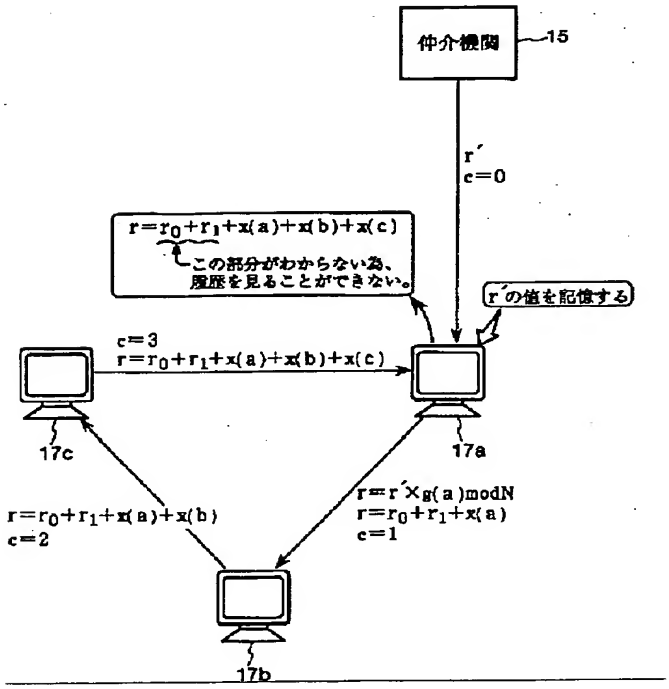


【図６】

〈電子マネー端末が単純にx(ｉ)を付加する場合〉



【図７】



【図８】